



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/806,772	03/23/2004	Trevor W. Freeman	M1103.70185US01	2366
45840 7590 12/26/2007 WOLF GREENFIELD (Microsoft Corporation) C/O WOLF, GREENFIELD & SACKS, P.C. 600 ATLANTIC AVENUE BOSTON, MA 02210-2206			EXAMINER HA, LEYNNA A	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 12/26/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/806,772

Applicant(s)

FREEMAN ET AL.

Examiner

LEYNNA T. HA

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 July 0102.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-23 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 18 recites the limitation "the public key pair of the DH key" in line 10.

There is insufficient antecedent basis for this limitation in the claim.

Throughout claim 18, recites a key pair comprising a public key and a private key. The claimed second network device receiving the public key of the key pair and then claims the second networked device using the public key of the DH key pair. The DH key pair cannot be considered or given as the received public key of the key pair or any other public key of the key pair recited in claim 18.

Response to Arguments

3. Applicant's arguments filed 10/2/07 have been fully considered but they are not persuasive.

Examiner traverses the argument on pg.7, that Balissat's approach uses three sets of messages that uses a separate set of messages for authentication which does not suggest all features of the claims. The features of the claims does not limit to a particular transmission or amount of messages being transmitted in the authentication

Art Unit: 2135

process. However, the key exchange (IKE protocol) broadly suggest a message sent to the initiator and a message sent to the responder where according to the claimed Diffie Hellman key pair is used to establish confidentiality and authentication. Hence, the claimed invention does suggest more than one transmission of data or messages because of the keys exchanged between the initiator and the responder is necessary to complete the authentication of the responder or initiator.

Examiner traverses the argument regarding claim 1 on pg.8, points to the claimed "the shared secret is used to authenticate the identity of the responder or the shared secret is used to authenticate the identity of the initiator". Applicant argues Balissat's process in which a separate set of messages is used for authentication does not suggest a method in claim 1. Examiner finds the number of messages used for authentication is irrelevant because the claimed invention does not limit to a single transmission of data, message, payload, or packet to authenticate the identity of the responder or the initiator. The claimed shared secret used to authenticate is merely referencing to a particular data being used for authentication. The claim broadly suggest the shared secret referring back to other separate instances where the shared secret is transmitted to the responder and an initiator created from the public and private DH key pair that was also exchanged between the responder and initiator. The creation of the shared secret is necessary for authentication since the shared secret was derived from the key pair exchanged between the responder and the initiator during the IKE negotiation to establish secure communications. Thus, the claimed suggests

Art Unit: 2135

exchanging multiple messages necessary to create the shared secret as part of the entire authentication process.

As for applying art in accordance to claim 1, Balissat discloses one device 100 seeks to initiate an SA with device 140 and IKE allows two devices to negotiate and agree on operations including establishment of the keys (col.7, lines 55-67). The messages described in Balissat's invention provides protection for the identity of the involved devices that may be between multiple peer devices (i.e. 1st device, 2nd device, firewall) and includes negotiating a pair of SAs (col.7, lines 21-25 and 54-57). However, each SA is only between two devices which suggests the encryption parameter (i.e. public and private keys) between the two devices corresponds to each other and particular to the two devices involved. For it is the same key pair that is used between the 1st device (initiator) and the 2nd device (responder) used in forwarding (encrypted) packets that is associated with authentication of a device by the establishment of security association SA (col.6, lines 60-64). Balissat also discusses allowing two users to build a symmetric secret key using their local private keys, a known DH key, and the other device's public key. A secret share key can be developed using the Diffie Hellman algorithm where two devices share a common secret key (col.9, lines 29-40 and 52-53). The secret key (shared, common, and symmetric) reads on the claimed shared secret. Therefore, Balissat reads on claim 1.

As for the arguments regarding claims 8 and 20 on pg.8, that Balissat neither show nor suggest the claimed the shared secret is used to authenticate the identity of the responder or the shared secret is used to authenticate the identity of the initiator.

Art Unit: 2135

Applicant did not explain further the reasons or provide evidence of the prior art.

Therefore, examiner can only disagree and traverse the argument by referring to the discussion above of claim 1.

As for the arguments regarding claim 15 on pg.8, Balissat does not teach or suggest that decryption of a message also authenticates the sender of the message. Balissat discloses IKE may authenticate a sender by the public key encryption also known as Diffie Hellman encryption. This involves each user generating a public and private key where the public key is sent to the other party such that when each user combines his own private key with the other's public key, they each obtain an identical secret key (shared secret). Balissat then discloses the first user can encrypt a message using the second user's public key and the second user will be able to decrypt the received message. In addition, the first user can use his private key to sign a message using the key pair to authenticate the transmitted message where the first user is authenticated to the second user as the one who sent the transmission (col.2, lines 43-62 and col.7, lines 55-63). Balissat considers the key pair as encryption parameter and the establishment of security association (SA) involves devices in a forwarding mechanism for packets. This suggests the key pair used in decrypting the message is the key pair associated to authenticating a device. Balissat discusses the SA describes operations that should be applied to future data packets including an authentication method, an encryption method, authentication/encryption keys and various other parameters (col.4, lines 23-65 and col.6, lines 60-67). Therefore, Balissat reads on the claimed a static DH key pair is used to establish confidentiality and authentication

Art Unit: 2135

whereby decryption of a message encrypted with the static DH key pair authenticates a device with the static key pair.

All other dependent claims remains rejected by virtue of their dependency.

4. Applicant's arguments with respect to claims 18-19 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claims 1-2, 4, 6-9, 11, and 13-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Balissat, et al. (US 7,188,365).**

As per claim 1:

Balissat discloses a method for establishing a secure communications channel and authenticating a party, for use by an initiator in an Internet Security Protocol (IPSec) negotiation (col.1, lines 43-54 and col.9, lines 22-27), comprising:

initiating an Internet Key Exchange (IKE) negotiation with a responder; **(col.2, lines 40-43 and col.8, lines 4-6)**

transmitting, to the responder, a public Diffie-Hellman (DH) key of the initiator; **(col.2, lines 45-48;** *device 100 is the claimed initiator and that device 100 can also be a firewall or gateway 110 (col.7, lines 57-59), but may also be the responder that exchange(s) with device 140 (col.10, lines 20-37). With either device being the initiator or responder, Balissat discloses both have a public DH key for exchange with each other (col.2, lines 45-48). By exchange keys to one another, Balissat suggests transmitting the initiator's public key to a responder and receiving from a responder the public key as claimed below. In addition, Balissat discloses in a Diffie-Hellman (DH) key exchange, two users to build a symmetric secret key (same key used for encryption and decryption) using their local private keys, a known DH key and the other device's public key (col.9, lines 27-33).*)

receiving, from the responder, a public DH key of the responder; **(col.9, lines 43-46;** *device 140 is referring to the claimed responder (col.8, lines 65-66) but may also be the one to initiate the exchange(s) and that the device 100 can be the responder (col.10, lines 20-32).*)

transmitting, to the responder, a payload encrypted **(col.7, lines 60-67)** with a shared secret created from the public DH key of the responder and the private DH key **(col.2, lines 48-55 and col.12, lines 14-16;** *Balissat discloses the encrypted payload or message with an identical (shared) secret key from the combined user's private key and the other's public key.)* corresponding to the public DH key of the initiator transmitted to the responder; **(col.9, lines 38-48 and col.10, lines 10-14)**

receiving, from the responder, a payload encrypted with the shared secret; and **(col.10, lines 2-8 and col.11, lines 23-27)**

decrypting the payload; (**col.13, lines 53-55**)

wherein the public DH key of the responder is a claim on the identity of the responder and the shared secret is used to authenticate the identity of the responder, or the public DH key of the initiator is a claim on the identity of the initiator and the shared secret is used to authenticate the identity of the initiator. (**col.2, lines 58-62 and col.3, lines 1-3**; *Balissat discloses the first user authenticated to the second user as the one who sent the transmission by using the private key to sign the message and the public key. Thus, the private key (shared secret key) is used authenticates the identity of the initiator. Balissat discloses the verifying the association of a public key with a particular user suggests the claimed public DH key is a claim on the identity of the initiator.)*

As per claim 2: See col.9, lines 38-67 and col.13, lines 15-23; discussing the method of claim 1 wherein the public DH key of the responder is previously known to the initiator and is a claim on the identity of the responder.

As per claim 4: See col.3, lines 1-13 and col.13, lines 15-23; discussing the method of claim 1 wherein the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator.

As per claim 6: See col.2, lines 13-15; discussing the method of claim 1 wherein the secure communications channel is a channel in a virtual private network (VPN).

As per claim 7: See col.2, lines 13-48; discussing the method of claim 6 wherein the VPN comprises a client and a server, and a public DH key of the VPN client is transmitted as a hint to the identity of the client.

Art Unit: 2135

As per claim 8:

Balissat discloses a method for establishing a secure communications channel and authenticating a party, for use by a responder in an Interact Security Protocol (IPSec) negotiation (**col.1, lines 43-54 and col.9, lines 22-27**), comprising:

receiving an Internet Key Exchange (IKE) negotiation request from an initiator;
(col.2, lines 40-43 and col.8, lines 4-6)

transmitting, to the initiator, a public Diffie-Hellman (DH) key of the responder;
(col.2, lines 45-48; device 100 is the claimed initiator and that device 100 can also be a firewall or gateway 110 (col.7, lines 57-59), but may also be the responder that exchange(s) with device 140 (col.10, lines 20-37). With either device being the initiator or responder, Balissat discloses both have a public DH key for exchange with each other (col.2, lines 45-48). By exchange keys to one another, Balissat suggests transmitting the initiator's public key to a responder and receiving from a responder the public key as claimed below. In addition, Balissat discloses in a Diffie-Hellman (DH) key exchange, two uses build a symmetric secret key (same key used for encryption and decryption) using their local private keys, a known DH key and the other device's public key (col.9, lines 27-33). Thus, this reads on the payload encrypted with a shared secret key claimed further below.)

receiving, from the initiator, a public DH key of the initiator; **(col.9, lines 43-46; device 140 is referring to the claimed responder (col.8, lines 65-66) but may also be the one to initiate the exchange(s) and that the device 100 can be the responder (col.10, lines 20-32).)**

Art Unit: 2135

transmitting, to the initiator, a payload encrypted (**col.7, lines 60-67**) with a shared secret created from the public DH key of the initiator and the private DH key (**col.2, lines 48-52**) corresponding to the public DH key of the responder transmitted to the initiator; (**col.9, lines 38-48 and col.10, lines 10-14**)

receiving, from the initiator, a payload encrypted with the shared secret; and (**col.10, lines 2-8 and col.11, lines 23-27**)

decrypting the payload; (**col.13, lines 53-55**)

wherein the public DH key of the responder is a claim on the identity of the responder and the shared secret is used to authenticate the identity of the responder (**col.3, lines 1-13**), or the public DH key of the initiator is a claim on the identity of the initiator and the shared secret is used to authenticate the identity of the initiator. (**col.12, lines 7-15 and col.13, lines 15-23**)

As per claim 9: See col.3, lines 1-13 and col.9, lines 38-67; discussing the method of claim 8 wherein the public DH key of the responder is previously known to the initiator and is a claim on the identity of the responder.

As per claim 11: See col.13, lines 15-23 and col.13, lines 15-23; discussing the method of claim 8 wherein the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator.

As per claim 13: See col.2, lines 13-15; discussing the method of claim 8 wherein the secure communications channel is a channel in a virtual private network (VPN).

As per claim 14: See col.2, lines 13-48 and col.13, lines 15-23; discussing the method of claim-13 wherein VPN comprises a client and a server, and a public DH key

Art Unit: 2135

of the VPN client is received as a hint to the identity of the client.

As per claim 15:

Balissat discloses a method of establishing, between an initiator and a responder (col.8, lines 65-67 and col.10, lines 20-32), a secure communications channel following the Internet Security Protocol (IPSec) (col.1, lines 43-54 and col.9, lines 22-27), comprising using the Internet Key Exchange (IKE) protocol (col.2, lines 40-43 and col.3, lines 1-13), wherein a static Diffie-Hellman (DH) key-pair (col.8, lines 4-6 and col.9, lines 25-46) is used by at least one of the initiator or the responder to establish confidentiality and authentication (col.7, lines 60-67 and col.13, lines 15-23)

whereby decryption of a message encrypted with the static Diffie-Hellman key-pair authenticates a device associated with the static key-pair. (col.4, lines 23-65 and col.6, lines 60-67; *Balissat discloses IKE may authenticate a sender by the public key encryption also known as Diffie Hellman encryption. This involves each user generating a public and private key where the public key is sent to the other party such that when each user combines his own private key with the other's public key, they each obtain an identical secret key (shared secret). Balissat then discloses the first user can encrypt a message using the second user's public key and the second user will be able to decrypt the received message. In addition, the first user can use his private key to sign a message using the key pair to authenticate the transmitted message where the first user is authenticated to the second user as the one who sent the transmission (col.2, lines 43-62 and col.7, lines 55-63). Balissat considers the key pair as encryption parameter and the establishment of security association (SA) involves devices in a*

Art Unit: 2135

forwarding mechanism for packets. This suggests the key pair used in decrypting the message is the key pair associated to authenticating a device. Balissat discusses the SA describes operations that should be applied to future data packets including an authentication method, an encryption method, authentication/encryption keys and various other parameters (col.4, lines 23-65 and col.6, lines 60-67).)

As per claim 16: See col.3, lines 1-13 and col.13, lines 15-23; discussing the method of claim 15 wherein the private DH key of the DH key-pair is used to create a claim of identity for the initiator or the responder.

As per claim 17: See col.2, lines 13-16; discussing the method of claim 15 wherein the secure communications channel is a channel in a virtual private network.

As per claim 20:

Balissat discloses a computer-readable medium including computer-executable instructions facilitating establishing a secure communications channel and authenticating a party, for execution by an initiator in an Internet Security Protocol (IPSec) negotiation (**col.1, lines 43-54 and col.9, lines 22-27**), said computer-executable instructions executing the steps of:

initiating an Internet Key Exchange (IKE) negotiation with a responder; (**col.2, lines 40-43 and col.8, lines 4-6**)

transmitting, to the responder, a public Diffie-Hellman (DH) key of the initiator; (**col.2, lines 45-48**; *device 100 is the claimed initiator and that device 100 can also be a firewall or gateway 110 (col.7, lines 57-59), but may also be the responder that exchange(s) with device 140 (col.10, lines 20-37). With either device being the initiator*

Art Unit: 2135

or responder, Balissat discloses both have a public DH key for exchange with each other (col.2, lines 45-48). By exchange keys to one another, Balissat suggests transmitting the initiator's public key to a responder and receiving from a responder the public key as claimed below. In addition, Balissat discloses in a Diffie-Hellman (DH) key exchange, two uses build a symmetric secret key (same key used for encryption and decryption) using their local private keys, a known DH key and the other device's public key (col.9, lines 27-33). Thus, this reads on the payload encrypted with a shared secret key claimed further below.)

receiving, from the responder, a public DH key of the responder; (col.9, lines 43-46; device 140 is referring to the claimed responder (col.8, lines 65-66) but may also be the one to initiate the exchange(s) and that the device 100 can be the responder (col.10, lines 20-32).)

transmitting, to the responder, a payload encrypted (col.7, lines 60-67) with a shared secret created from the public DH key of the responder and the private DH key (col.2, lines 48-52) corresponding to the public DH key of the initiator transmitted to the responder; (col.9, lines 38-48 and col.10, lines 10-14)

receiving, from the responder, a payload encrypted with the shared secret; and (col.10, lines 2-8 and col.11, lines 23-27)

decrypting the payload; (col.13, lines 53-55)

wherein the public DH key of the responder is a claim on the identity of the responder and the shared secret is used to authenticate the identity of the responder (col.3, lines 1-13), or the public DH key of the initiator is a claim on the identity of the

Art Unit: 2135

initiator and the shared secret is used to authenticate the identity of the initiator. (**col.12, lines 7-15 and col.13, lines 15-23**)

As per claim 21: See col.9, lines 38-67 and col.13, lines 15-23; discussing the computer-readable medium of claim 20 wherein the public DH key of the responder is previously known to the initiator and is as a claim on the identity of the responder.

As per claim 22: See col.3, lines 1-13 and col.13, lines 15-23; discussing the computer-readable medium of claim 20 wherein the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator.

As per claim 23: See col.2, lines 13-16; discussing the computer-readable medium of claim 20 wherein the secure communications channel is a channel in a virtual private network.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 3, 5, 10, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balissat, et al. (US 7,188,365), and further in view of Hur (US 7,181,620).

As per claim 3: Balissat discloses the method of claim 4 wherein a responder comprises a computing device and has previously obtained the public DH key of the initiator (col.9, lines 27-48) separate from and connectable to the computing device but fails to include from a portable media device separate from and connectable to the computing device.

Hur discloses the system may be used to provide distributed key management for secure configuration or provisioning of network devices that are applicable to any multimedia terminal adapter, routers, gateways, etc. (col.8, lines 47-58). The term device is also a peer and peers can be switches, workstations, servers, etc. (col.11, lines 23-35). Hur discusses the key pair stored in directory server (col.11, lines 10-20) or the key management server and that secure storage may be smart cards or token cards, locally encrypted storage, a directory server, or removable media (col.4, lines 63-66 and col.18, lines 33-55). Thus, Hur suggests the public key can be stored in a portable media device with is a computer-readable media that are accessible to the programmatic elements (col.11, lines 1-3 and col.17, lines 45-52).

Therefore, it would have bee obvious for a person of ordinary skills in the art to combine the teaching of Balissat with Hur to teach a portable media device separate from and connectable to the computing device because is a computer-readable media for secure storage may be smart cards or token cards, locally encrypted storage, a

Art Unit: 2135

directory server, or removable media (Hur -col.4, lines 63-66 and col.18, lines 33-55) that are accessible to the programmatic elements (Hur -col.11, lines 1-3 and col.17, lines 45-52).

As per claim 5: Balissat discloses the method of claim 4 wherein the initiator comprises a computing device and has previously obtained the public DH key of the responder (col.9, lines 27-48 and col.10, lines 5-14) but fails to include from a portable media device, separate from and connectable to the computing device.

Hur discloses the system may be used to provide distributed key management for secure configuration or provisioning of network devices that are applicable to any multimedia terminal adapter, routers, gateways, etc. (col.8, lines 47-58). The term device is also a peer and peers can be switches, workstations, servers, etc. (col.11, lines 23-35). Hur discusses the key pair stored in directory server (col.11, lines 10-20) or the key management server and that secure storage may be smart cards or token cards, locally encrypted storage, a directory server, or removable media (col.4, lines 63-66 and col.18, lines 33-55). Thus, Hur suggests the public key can be stored in a portable media device with is a computer-readable media that are accessible to the programmatic elements (col.11, lines 1-3 and col.17, lines 45-52).

Therefore, it would have bee obvious for a person of ordinary skills in the art to combine the teaching of Balissat with Hur to teach a portable media device separate from and connectable to the computing device because is a computer-readable media for secure storage may be smart cards or token cards, locally encrypted storage, a directory server, or removable media (Hur -col.4, lines 63-66 and col.18, lines 33-55)

Art Unit: 2135

that are accessible to the programmatic elements (Hur -col.11, lines 1-3 and col.17, lines 45-52).

As per claim 10: Balissat discloses the method of claim 9 wherein the responder comprises a computing device and has previously obtained the public DH key of the initiator (col.9, lines 27-48) but fails to include from a portable media device, separate from and connectable to the computing device.

Hur discloses the system may be used to provide distributed key management for secure configuration or provisioning of network devices that are applicable to any multimedia terminal adapter, routers, gateways, etc. (col.8, lines 47-58). The term device is also a peer and peers can be switches, workstations, servers, etc. (col.11, lines 23-35). Hur discusses the key pair stored in directory server (col.11, lines 10-20) or the key management server and that secure storage may be smart cards or token cards, locally encrypted storage, a directory server, or removable media (col.4, lines 63-66 and col.18, lines 33-55). Thus, Hur suggests the public key can be stored in a portable media device with is a computer-readable media that are accessible to the programmatic elements (col.11, lines 1-3 and col.17, lines 45-52).

Therefore, it would have bee obvious for a person of ordinary skills in the art to combine the teaching of Balissat with Hur to teach a portable media device separate from and connectable to the computing device because is a computer-readable media for secure storage may be smart cards or token cards, locally encrypted storage, a directory server, or removable media (Hur -col.4, lines 63-66 and col.18, lines 33-55)

Art Unit: 2135

that are accessible to the programmatic elements (Hur -col.11, lines 1-3 and col.17, lines 45-52).

As per claim 12: Balissat discloses the method of claim 11 wherein the initiator has previously obtained the public DH key of the responder (col.9, lines 27-48 and col.10, lines 5-14) but fails to include from a portable media device.

Hur discloses the system may be used to provide distributed key management for secure configuration or provisioning of network devices that are applicable to any multimedia terminal adapter, routers, gateways, etc. (col.8, lines 47-58). The term device is also a peer and peers can be switches, workstations, servers, etc. (col.11, lines 23-35). Hur discusses the key pair stored in directory server (col.11, lines 10-20) or the key management server and that secure storage may be smart cards or token cards, locally encrypted storage, a directory server, or removable media (col.4, lines 63-66 and col.18, lines 33-55). Thus, Hur suggests the public key can be stored in a portable media device with is a computer-readable media that are accessible to the programmatic elements (col.11, lines 1-3 and col.17, lines 45-52).

Therefore, it would have bee obvious for a person of ordinary skills in the art to combine the teaching of Balissat with Hur to teach a portable media device separate from and connectable to the computing device because is a computer-readable media for secure storage may be smart cards or token cards, locally encrypted storage, a directory server, or removable media (Hur -col.4, lines 63-66 and col.18, lines 33-55) that are accessible to the programmatic elements (Hur -col.11, lines 1-3 and col.17, lines 45-52).

Art Unit: 2135

7. Claims 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hur (US 7,181,620) , and further in view of Balissat, et al. (US 7,188,365).

As per claim 18:

Hur discloses a system for establishing a secure communications channel between networked devices connected over a network, the system comprising:

a first networked device generating a key pair, the key pair comprising a public key and a private key; (col.11, lines 9-12 and ; Hur discloses a communicating device is also considered as a peer or device 510A as the claimed first networked device (col.13, lines 8-10).)

a portable media device storing the public key of the pair generated by the first networked device; and (col.11, lines 1-3 and col.17, lines 45-52; Hur discloses the system may be used to provide distributed key management for secure configuration or provisioning of network devices that are applicable to any multimedia terminal adapter, routers, gateways, etc. (col.8, lines 47-58). The term device is also a peer and peers can be switches, workstations, servers, etc. (col.11, lines 23-35). Hur discusses the key pair stored in directory server (col.11, lines 10-20) or the key management server and that secure storage may be smart cards or token cards, locally encrypted storage, a directory server, or removable media (col.4, lines 63-66 and col.18, lines 33-55). Therefore, Hur suggests the public key can be stored in a portable media device.)

a second networked device receiving the public key of the key pair over the network as part of an exchange of message (col.16, lines 39-64) establishing an IPsec security association and reading the public key of the key pair from the portable media device; (col.9, lines 20-42 and col.15, lines 1-3)

the second networked device using the public key of the DH key pair to ensure confidentiality and authenticity in securing a communications channel with another networked device, following the Internet Key Exchange (IKE) and Internet Security (IPSec) protocols, (col.15, lines 6-13 and col.16, line 65 – col.17, line 3)

wherein the portable media device is separate from the network and from the first and second networked devices and is connectable to the second networked device. (col.15, lines 49-52)

Hur discloses the invention of initial peer-to-peer security phase establishes a session key between two peers in a network (col.14, lines 61-64) that could be used to establish a key for use in encrypting a flow of packets among peer routers in a packet-switched network under the IPSec protocol (col.15, lines 1-3). However, the embodiment then enable two message exchange for generating keys for IPSec security associations as opposed to a six message exchange as required using the Internet Key Exchange (IKE) protocols (col.15, lines 10-13). Although, Hur discusses the IKE protocol, but did not implement IKE protocol.

Balissat discloses a method for implementing secure network communications between a first device and a second device, at least one of the devices communicating with the other device via a separate computer (col.4, lines 22-30). Balissat discloses

Art Unit: 2135

the separate computer is a device that may be a gateway, router, or firewall device (col.7, lines 55-59). Similar to prior art Hur, Balissat teaches the device 100 (first network device) seeks to initiate with device 140 (second network device) where devices 100 and 140 establish a secret key together via the first SA and then uses the public key of the firewall 110 (col.7, lines 24-26). Thus, reads on the claimed the second device receiving from the portable device the public key of the key pair. Balissat discusses initiating a session in negotiating an SA using IKE (col.8, lines 4-6) and the SA operations applied to packets include an authentication method, encryption method, and authentication/encryption keys where IKE allows two devices to negotiate and agree on these operations including establishment of the keys (col.7, lines 60-67). Balissat further explains the IKE typically operates in two phases, a first phase is where parties agree as to how to protect further negotiation traffic (i.e. IKE may authenticate a sender by Diffie-Hellman encryption) and the second phase is where IKE negotiates the actual IPsec SA by setting up the encryption/authentication keys for the AH and/or ESP protocols (col.2, lines 40-52 and col.3, lines 10-12). Balissat discusses a particular conventional protocol for providing security between devices operating over an Internet Protocol (IP) network is known as IPsec. IPsec is a set of protocols supporting the secure exchange of IP packets at a network layer (col.1, lines 48-52).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Hur with Balissat to teach Internet Key Exchange (IKE) and Internet Security (IPSec) protocols because IKE parties agree as to how to protect further negotiation traffic negotiates and the actual IPsec SA by setting up the

Art Unit: 2135

encryption/authentication keys for the AH and/or ESP protocols (Balissat – col.2, lines 40-52 and col.3, lines 10-12) and IPsec protocol is a conventional protocol for providing security between devices operating over an Internet Protocol (IP) network that supports the secure exchange of IP packets at a network layer (Balissat – col.1, lines 48-52).

As per claim 19: See Balissat on col.2, lines 13-16; discussing the system of claim 18 wherein the secure communications channel is a channel in a virtual private network.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

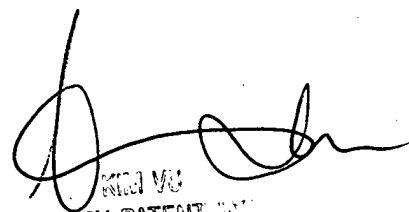
Art Unit: 2135

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

A handwritten signature in black ink, appearing to be 'Kim Vu', written over a faint, partially legible stamp that includes the words 'PATENT' and 'EXAMINER'.